Published and Copyright (c) 1999 - 2016
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1815 04/15/16

~ Millions Still Run XP! ~ People Are Talking! ~ Experts Crack Petya!
~ Rollercoaster Tycoon! ~ "Punch-Out" Easter Egg ~ A New Ransomware!
~ More Ghostbusters Soon ~ Apple Going xxxOS Path ~ Facebook Account Kit!

~ Some Modems Vulnerable ~ ~ OS X Gets Re-branded?

-* Uninstall Apple QuickTime Now *-
-* URL Shorteners, Convenient & Risky! *-
-* Microsoft Edge Becomes Ad-blocker, of Sort *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

This week flew by! Here we are on the unofficial day for taxes! Well, actually, not this year due to a holiday being celebrated in Washington, D.C. So, that means the deadline for filing your taxes has been extended until Monday. And, if you live in Massachusetts, that deadline has been extended to Tuesday because of Patriots Day!

So, if you're a tax-filing procrastinator like I am, you still have a few more days to finish up your tax returns and get them in the mail (literally or electronically). I filed mine last weekend, finally.

Until next time...

=~=~=~=

->In This Week's Gaming Section - Two New Ghostbusters Video Games Coming Soon!
""""""""""""""""""""""""""""""" Mike Tyson's Punch-Out!! Still Has Secrets!
Atari: Won't Walk Away from Rollercoaster!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Two New Ghostbusters Video Games Coming Soon From Activision

With the Ghostbusters reboot tiptoeing nearer and nearer, the marketing machine is in full swing, with Activision announcing via that they have not one, but two upcoming games in production.

The first is a four-player RPG simply titled Ghostbusters, which serves as a sequel to the reboot film featuring a new cast of characters keeping ghosts at bay in New York City. Check out the trailer below ahead of its July 12 for PS4, Xbox One, and PC.

The other is a mobile game called Ghostbusters: Slime City, which also launches in July, and has you teaming up with other Ghostbusters to again protect NYC from supernatural threats.

From the Press Release:

Activision Publishing, Inc., in collaboration with Sony Pictures Consumer Products, has announced a pair of new Ghostbusters video games set in and inspired by the comedic action world of the upcoming Ghostbusters film, in theaters July 15. Taking place after the events of the new movie, both Ghostbusters games introduce new casts of rookies keeping watch over the station while the now-famous Ghostbusters tour the country stopping high-profile poltergeists. When paranormal phenomena unleash apparitions across New York City, these new squads of recruits must don their proton packs and wrestle those rogue spirits back to the afterlife!

The console game, Ghostbusters, is a third-person action role-playing game positively charged for thrilling couch co-op with up to four players locally. As rookie Ghostbusters, players can level up their characters  gear and abilities by tackling objectives, defeating ghastly creatures and discovering hidden collectibles in Manhattan s most haunted haunts. There are four heroes to choose from, and each has his or her own unique personality and play style, bringing special strengths to support the team.

Ghostbusters is expected to arrive on the PlayStation4 computer entertainment system, Xbox One and Windows PC via Steam on July 12.

The mobile game, Ghostbusters: Slime City, lets players be a Ghostbuster and save New York City from a new wave of threats. Team up with other players in asynchronous co-op, and collect powerful ghosts to rise to the top of the leaderboards. Players can also craft their own proton packs from any number of combinations of components, as well as upgrade their own headquarters and complete jobs around the city for new weapons and rewards.

Ghostbusters: Slime City is expected to launch in July on select iPhone, iPad and iPod touch devices via the App Store, select Android devices via Google Play and select Kindle devices through the Amazon Appstore.

## Atari: We Won’t Walk Away from Rollercoaster Tycoon World

It may have received a critical mauling, but Atari says it s not about to give up on its new Rollercoaster Tycoon game.

The CEO of Atari says Rollercoaster Tycoon World is already

looking and playing better than it was a week ago, and that there are 55 full-time staff working on the project  a number that rises to around 80 when you factor in contractors.

Rollercoaster Tycoon World has gone through multiple developers and was due to arrive at the end of 2015. It finally turned up on Steam s Early Access - a platform for unfinished titles - last month, with the user reviews being  mostly negative .

 We have had a number of negative reactions from launch,  said Atari CEO Frederic Chesnais.  But if you look at the number of concurrent users  people playing the game  I think it is pretty good. It s a long run, this isn t a hit and run project, we re not about to walk away. There is a lot to come, and we have a post-launch plan to introduce new features.

One of the game s criticisms focused on its low quality visuals, and Chesnais says this was due to the team being nervous about the game s performance.

 I take the blame on that,  he said.  We were just a bit shy and afraid of things like frame rates. Before we launched Rollercoaster Tycoon World we were receiving feedback about frame rate issues that we weren t seeing on our end sometimes. So we thought there might be a disconnect and that perhaps we were asking too much from players in terms of performance from their computers. So I said let s put the focus on performance over the visual quality.

 We could have released the game in 4K, but we decided to go in the direction of performance over visual quality. I think the balance hasn t been right, so that is why we have effectively reversed it with our latest update.

He added that the firm has read all the online reviews, although not all of them have been helpful.

Chesnais added:  If you work two years on a project and love your game, and then you release it and you have positive and negative reviews and other reviews  and by  other  I mean people who trash the game even if they ve barely played it  then, well, you have to love your job, right?

 What I want to say is that we do read what people are writing. Even if it is positive or negative, we look at it and work out how to make the game better. We do read all the reviews. We do care.

=~=~=~=

->A-ONE Gaming Online  -  Online Users Growl & Purr!
  """""""""""""""""""""

Mike Tyson’s Punch-Out!! Still Has Secrets To Share, 29 Years Later

Nearly 30 years after Mike Tyson’s Punch-Out!! launched on the Nintendo Entertainment System, gamers are still discovering secrets inside it.

As Redditor midwesternhousewives discovered, there is a visual cue among the spectators in the second Piston Honda fight, which tells the player when to throw a punch that knocks Honda out with one blow. A one-punch KO of Honda has been known for years, though gamers were left to guess exactly when that window is open during his special attack. Now it’s clear; just watch the bearded guy on the front row, about seven over from the left.

Another user in the Reddit thread describing the tip-off notes that "the bearded man did not flinch or move a single pixel until I reached the second fights with piston Honda and bald bull."

The same spectator provides the same tip-off during Bald Bull’s notorious charge attack in his second fight, which also can be stopped with one punch. When beardy ducks. blast Bull with a body blow, and its bedtime for Baldy.

In the first Bald Bull bout, a camera flash signals the time to throw the punch; that was revealed in 2009 by the late Satoru Iwata in one of the Nintendo president’s roundtables with Punch-Out!!’s creators.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

## Experts Crack Petya Ransomware

Security experts have devised a method that allows users to recover data from computers infected with the Petya ransomware program without paying money to cybercriminals.

Petya appeared on researchers’ radar last month when criminals distributed it to companies through spam emails that masqueraded as job applications. It stood out from other file-encrypting ransomware programs because it overwrites a hard disk drive’s master boot record (MBR), leaving infected computers unable to boot into the operating system.

The program replaces the drive’s legitimate MBR code, which normally starts the operating system, with code that encrypts the master file table (MFT) and shows a ransom note. The MFT is a special file on NTFS volumes that contains information about all other files: their name, size and mapping to hard disk sectors.

The actual contents of the user’s files are not encrypted, but

without the MFT, the OS no longer knows where those files are located on disk. Using data recovery tools to reconstruct files might be possible, but it is not guaranteed to work perfectly and would be time-consuming.

Fortunately, resorting to that method is no longer necessary, and neither is paying Petya's authors. Someone using the online handle leostone devised an algorithm to crack the key needed to restore the MFT and recover from a Petya infection.

Computer experts from the popular tech support forum BleepingComputer.com confirmed that the technique works, but it requires extracting some data from an affected hard drive: 512 bytes starting at sector 55 (0x37h) with an offset of 0 and an 8-byte nonce from sector 54 (0x36) offset 33 (0x21).

If that sounds complicated, no worries: Fabian Wosar from security firm Emsisoft created a simple and free tool that can do it for you. However, because the infected computer can no longer boot into Windows, using the tool requires taking out the affected hard drive and connecting it to a different computer where the tool can run. An external, USB-based hard drive docking station can be used.

The data extracted by the tool must be inputted into a Web application created by leostone that will use it to crack the key. The user must then put the affected hard drive back into the original computer, boot from it, and input the key on the ransom screen displayed by Petya.

"Once the hard drive is decrypted, the ransomware will prompt you to reboot your computer and it should now boot normally," BleepingComputer.com founder Lawrence Abrams, wrote in a blog post.

## No Password Required! 135 Million Modems Open to Remote Factory Reset

More than 135 Million modems around the world are vulnerable to a flaw that can be exploited remotely to knock them offline by cutting off the Internet access.

The simple and easily exploitable vulnerability has been uncovered in one of the most popular and widely-used cable modem, the Arris SURFboard SB6141, used in Millions of US households.

Security researcher David Longenecker discovered a loophole that made these modems vulnerable to unauthenticated reboot attacks. He also released his "exploit" after Arris (formerly Motorola) stopped responding to him despite a responsible disclosure.

The Bug is quite silly: No Username and Password Protection.

Arris does not provide any password authentication set up on the modem s user interface, thus allowing any local attacker to access the administration web interface at 192.168.100.1 without the need to enter a username and password.

This issue allows a local attacker to 'Restart Cable Modem' from

the ’Configuration page’ of the administrative interface at http://192.168.100.1/, as shown. This is nothing but a Denial of Service (DoS) attack.

Bingo! By clicking ’Restart Cable Modem’ manually will disable victim’s modem for 2 to 3 minutes and every device on that network will lose access to the Internet.

However, three minutes of no Internet connectivity is bearable, but the same administrative panel provides an option to Factory Reset the modem as well i.e. wipe out modem’s configuration and settings.

If an attacker clicks this option, your modem will go offline for 30 minutes as re-configuration process takes as long as an hour to complete. Though, sometimes you need to call your Internet Service Provider (ISP) to reactivate the modem.

David revealed that an attacker can also reset your modem remotely, as the application doesn’t verify whether the reboot or reset the modem command comes from the UI interface or an external source.

This remote attack is known as a Cross-Site Request Forgery (CSRF) attack that allows an attacker to use social engineering techniques to trick users into clicking on a specially crafted web page or email.

For example: A web page including <img src="http://malicious_url/"> tag could call any of the following URLs:

http://192.168.100.1/reset.htm (for restart)
http://192.168.100.1/cmConfigData.htm?BUTTON_INPUT1=Reset+All+Defaults (for factory reset)

"Did you know that a web browser does not care whether an ’image’ file is really an image?," Longenecker explains. "Causing a modem to reboot is as simple as including an ’image’ in any other web page you might happen to open."

"Of course, it is not a real image, but the web browser does not know that until it requests the file from the modem IP address which of course causes the modem to reboot."

However, these flaws are easily patchable that only requires Arris to create a firmware update such that:

The UI requires authentication (username and password) before allowing someone to reboot or reset the modem.
The UI validates that a request originated from the application and not from an external source.

However, the bad news is that there’s no practical fix for the flaws. Since cable modems are not consumer-upgradable, even if Arris releases a fix, you would need to wait for your ISPs to apply the fix and push the update to you.

Arris has recently addressed the flaws with a firmware update.

"We are in the process of working with our Service Provider

customers to make this release available to subscribers," said the company’s spokesperson.

"There is no risk of access to any user data, and we are unaware of any exploits. As a point of reference, the 135 million number is not an accurate representation of the units impacted. This issue affects a subset of the ARRIS SURFboard devices."

## Meet The New Ransomware That Knows Where You Live

There’s a new malware attack in town, and it’s designed to hit a little too close to home.

A new phishing campaign is sending thousands of ominous-looking emails that contain the recipient’s home address.

The well-worded email appears to come from a legitimate email address and domain name, and raises very few irregularities. The email comes with an demand for money for an arbitrary service, along with a link that purports to be an "overdue invoice."

Click that link and open the file (which looks like a Word document), and you’ll become the latest victim of ransomware - that is, malware that encrypts your files and locks you out of your computer until you pay a ransom.

The longer you wait, the larger the ransom you have to pay.

We received an email on Wednesday, which included my home address from some eight years earlier. Besides a tweet noting the phishing effort, we didn’t think much more of it.

But then the BBC News also reported that some of their staffers had also received similar looking emails.

We contacted the company named in our email which demanded money that was purportedly owed.

"We’re just as much victims as those who got the emails," said a person at the company who we spoke with on the phone. The Ludlow, UK-based company said that they began receiving phone calls and emails earlier this week, but stressed that the phishing emails were not from the company.

A number of other companies were implicated by the scam. BBC reports that other companies had "more than 150 calls from people who don’t owe us money."

The company said it had no idea how the scammers got people’s home addresses, but said they had reported the incident to police.

Rahul Kashyap, executive vice-president and chief security architect at security firm Bromium, said in an email that the scammer was using a "classic social engineering" technique by trying to "gain credibility by providing some reliable data that the potential victims can relate to."

"It appears that the scammers are leveraging some sort of database that has home addresses publicly available and using this for the scam," said Kashyap.

Scammers are increasingly moving away from enticing victims into entering their username and passwords on fake websites in order to take over accounts.

They're now turning to ransomware which has a much higher return.

In tests in CNET's lab in New York, we verified that the malware used in this ransomware attack is a variant called Maktub Locker, described as a "beautiful and dangerous" kind of ransomware.

Yonathan Klijnsma, a senior threat intelligence analyst at Dutch security firm Fox-IT, said that the fact the malware doesn't need an internet connection is "pretty significant," not least because network detection systems wouldn't be effective.

"It means you can retrieve your mail, step on a plane, open your mail and still get hit," he explained.

Ransomware is increasingly becoming problematic for private companies and citizens alike.

The FBI said last year that one popular variant of ransomware has cost businesses tens of millions in damages for lost files.

Many hospitals, in particular, have faced shutdowns and declared emergencies when their systems were hit by file locking malware. More recently, the federal agency called on US businesses in a flash advisory to help agents investigate the ever-growing kind of malware.

## Uninstall Now! Apple Abandons QuickTime for Windows

Yet another program is joining Java 6 and Windows XP as big-name software you do not want running on your PC. Security firm Trend Micro and the U.S. Department of Homeland Security are advising all Windows users to uninstall Apple s QuickTime as soon as possible. (The advisory does not affect Mac users.)

The reason for getting rid of QuickTime for Windows is twofold. First, Apple told Trend Micro it is deprecating the software and will no longer deliver security updates for it. Second, there are two known critical vulnerabilities that could allow an attacker to take control of a system running QuickTime.

That's a hellacious combo.

Apple was unavailable for comment at this writing, but a quick look at QuickTime s download page shows the software is still publicly available. It hasn t been updated since at least January, however.

Trend Micro says it does not yet know of any instances where the

two potential security threats are being used in the wild but that could change. Trend Micro s Zero Day Initiative recently published some technical details about the vulnerabilities. ZDI did this because its disclosure policy requires it to publish threat information when a vendor indicates that the product is deprecated, and thus won t be patched.

If you're a longtime user of iTunes you may be running QuickTime. To dump the program, open the Control Panel on your PC and then from the category view go to Programs > Uninstall a program. Once the list of installed programs populates, scroll down until you find QuickTime. Select it with your mouse, and then click Uninstall towards the top of the window. A pop-up window will then appear asking to confirm that you want to uninstall the program. Click Yes and you ll be QuickTime-free in no time.

A survey published by Secunia Research in late 2015 found that Apple software is among the programs that are updated the least often by Windows users.

Why this matters: Whenever software is about to be abandoned it s always a good idea to move away from it or at least start planning to. That goes double for software with known flaws that allow the bad guys to execute code on your machine. QuickTime used to be an important piece of software for Windows users. But these days you don t need it to watch movie trailers on Apple s site and it's no longer used by iTunes to play media on Windows. There s little reason for the vast majority of Windows users to keep QuickTime on their PCs.

## Microsoft Edge Becomes An Adblocker Of Sorts

Microsoft is following what Apple did with Safari back in 2013, and Google did with Chrome in 2015.

Simply put, the Edge browser will as good as block Flash ads by default.

Of course, that s not exactly what Microsoft is doing, nor is it quite how Microsoft has described the feature.

It s not about security, even though Microsoft s announcement starts off with:

> One of our top priorities in building Edge has been that the web should be a dependably safe, performant, and reliable place for our customers.

Nor is it really about turning Edge into an adblocker after all, ads are vital to Microsoft s business, just as they are to Apple and Google.

Apple pitched Safari s Flash-blocker as the Safari Power Saver; Google announced its Flash regulator under the headline Better battery life for your laptop; and Microsoft is following suit (our emphasis):

> We re introducing a change to give users more control over the power and resources consumed by Flash.

Ads will still be loaded, but Flash content that isn t considered central to the web page you re on will be  auto-paused,  meaning that you ll have to click on the content before it starts playing.

Microsoft doesn t define how it decides what counts as  central, but we imagine that the algorithm will use some combination of where the Flash came from, thus penalising third-party content sucked down from an ad network, and where it will be displayed, thus penalising animations around the edge of the page:

> Peripheral content like animations or advertisements built with Flash will be displayed in a paused state unless the user explicitly clicks to play that content. This significantly reduces power consumption and improves performance while preserving the full fidelity of the page. Flash content that is central to the page, like video and games, will not be paused.

In other words, Microsoft, like Apple and Google before it, isn t admitting that having the Flash plugin in your brower might be a security risk, and it isn t jumping into the argument about whether the online ad industry is out of control or not.

It s mostly about battery life.

Ironically, uninstalling Flash isn t enough to eliminate ads these days.

Amazon, for example, banned Flash ads from September 2015, but apparently as a way to make ads more likely to appear, given the ever-increasing popularity of blocking browser-based Flash:

> [Amazon s ban on flash ads] ensures customers continue to have a positive, consistent experience across Amazon and its affiliates, and that ads displayed across the site function properly for optimal performance.

What to do?

Like you, we ve noticed how power-hungry Flash content can be (if you live in a warm climate, your laptop fans can be a handy early-warning system for battery-sapping web pages), so Microsoft s announcement is a welcome one.

Nevertheless, we re sticking to our recommendation to try turning Flash off, and uninstalling it altogether if that works for you.

Indeed, we re not yet sure how much protection Edge s  auto-pause is likely to give you against deliberately-poisoned ads, because the ads will still be loaded, which implies that some Flash code in the ads might get to run anyway, even if it doesn t get to run for long before it gets paused.

With two zero-day patches in two months, and ever-fewer sites that actually need Flash, we think it s a potential security risk that you d do better to eliminate altogether if you can, rather than simply skating around it.

# URL Shorteners: Convenient But A Potential Security Risk

Services that shorten URLs can be great. They help take a giant, messy, unwieldy string of text and make it a lot more manageable.

Unfortunately, some short URLs also have one major flaw: if the URL is tiny enough, they're pretty easy to guess. In most instances that doesn't matter; maybe you're just shortening an online article URL to share on Twitter. However, two security researchers published a paper yesterday that details how Microsoft's OneDrive and Google's Maps services are easily exploited by this method.

As Ars Technica reports, the URL shorteners these companies use to give users direct links to files, addresses, or directions are simply too short. Said researchers brute-forced a ton of different links and then used them as starting points for accessing the rest of a user's data or, in the case of Google Maps, a user's identity.

With OneDrive, the researchers scanned 100 million different six-digit bit.ly URLs which map directly to the "1drv.ms" URL shortener Microsoft uses for OneDrive. Of these URLs, 42 percent were live, and 19,524 linked to OneDrive files (mostly live).

"OneDrive URLs have predictable structure. From the URL to a single shared document ("seed"), one can construct the root URL and automatically traverse the account, discovering all files and folders shared under the same capability as the seed document or without a capability," reads a blog post from one of the researchers, Cornell Tech professor Vitaly Shmatikov.

"The traversal-augmented scan yielded URLs to 227,276 publicly accessible OneDrive documents, including dozens of thousands of PDF and Word files, spreadsheets, media files, and executable binaries. A similar scan of 100,000,000 random seven-character bit.ly tokens yielded URLs to 1,105,146 publicly accessible OneDrive documents. We did not download their contents, but just from the metadata it is obvious that many of them contain private or sensitive information," he added.

Worse, around 7 percent of OneDrive folders the researchers found using this method had full write access. So, presumably, a person could easily dump malware into the folder, which would then synchronize to a person's various OneDrive-connected devices.

As for Google Maps, the researchers found just under 24 million live links when they scanned various five-digit permutations of shortened Google Maps URLs. Around 10 percent were links to maps with driving directions.

"The endpoints of driving directions often contain enough information (e.g., addresses of single-family residences) to uniquely identify the individuals who requested the directions. For instance, when analyzing one such endpoint, we uncovered the address, full name, and age of a young woman who shared directions

to a Planned Parenthood facility. Conversely, by starting from a residential address and mapping all addresses appearing as the endpoints of the directions to and from the initial address, one can create a map of who visited whom," Shmatikov wrote.

Though Microsoft has said that these issues are not themselves security vulnerabilities surprisingly it has since disabled bit.ly-based URL shortening within OneDrive. It also changed its URL structures to prevent digging through a person's other shared data from one successful shortened URL. As for Google, the company has switched to much longer tokens for its shortened URLs, greatly increasing the difficulty of brute-forcing live ones.

"We're continually looking for ways to improve the usability, features and security of our products and services for customers. As part of these efforts, earlier this year we began removing shortened URLs from file sharing options to simplify for users and prepare for future developments," Microsoft told Wired.

Google told Wired the company "appreciate[s] [the Cornell Tech researchers] contributions to the safety of Google Maps and other Google products. The Cornell researchers notified us last year about this issue and we've since strengthened URL protections based on their findings and our own studies."

## Millions of People Are Still Running Windows XP

It s been two years since Microsoft ended support for Windows XP, the popular operating system that s been around since 2001 and which many people just don t seem willing to let go.

Microsoft did about all it could to drag XP-ers into the present with pop-up warnings urging them that they need to upgrade, and a free migration tool to help people transfer their files and settings to Windows 7 or Windows 8.

It s not merely that Microsoft wants to get everybody onto the latest version of Windows, although it has certainly gone to great lengths recently to get people to upgrade to Windows 10, whether they want to or not.

But as we at Naked Security repeatedly warned XP users, the end of support means zero-days forever, because those vulnerabilities will never be patched and XP computers are sitting ducks for cybercriminals to attack.

And yet there are still millions of XP computers connecting to the internet, where all manner of malware is waiting to pounce.

Windows XP was still running on 10.9% of all desktops as of March 2016, according to stats compiled by Net Applications.

To put that in perspective, according to Net Applications figures, Windows XP is still the third-most popular desktop OS, trailing only Windows 7 (51.9%) and Windows 10 (14.2%).

And there are more PCs running XP than Windows 8.1 (9.6%), and all versions of Mac OS X combined (7.8%).
Desktop OS market share, March 2016 (source: Netmarketshare.com).

By the way, there are some Mac OS X users who are using out-of-support versions, too, meaning they are also vulnerable to never-going-to-be-fixed security holes.

Net Applications  stats show that just under 1% of all desktops are running OS X 10.6 (Snow Leopard), 10.7 (Lion) or 10.8 (Mountain Lion), which are no longer receiving security updates from Apple.

Things look slightly better when you look at OS market share measured by a different company, Stats Counter, but there s still an alarming number of PCs running XP.

According to Stat Counter, Windows XP represents 7.4% of all desktops in April 2016, down from 10.9% in April 2015.

That s an improvement.

But when you consider that Microsoft puts the number of Windows devices at more than 1 billion, we are still talking about tens of millions of computers today running a very old, very outdated, and very insecure operating system.

## Facebook Hopes To Kill The Username and Password

At its F8 developer conference, Facebook announced Account Kit, a new way for app developers to let users sign up for services with an email or phone number, no username or password required.

An extension of the existing Facebook login system, Account Kit is designed for developers who want an easy way for users to create accounts without having to sign in using Facebook.

Account Kit lets developers drop in code that will speed up the account-creation process. Instead, a user can use an email address or phone number. Users will receive a confirmation message via SMS or email to get setup.

If this sounds a lot like Digits  which is part of Twitter s Fabric development platform  that s because it is.

The idea is to reduce the friction it takes to sign up for an account within an app. And although we re sure Facebook would prefer that users sign up for an app with a Facebook account (app developers would probably prefer that too), solving the problem of user sign-ups is important. And if Account Kit can help with that, it ultimately means more developers are using Facebook s developer tools and platforms.

Account Kit is available for iOS, Android and web and mobile web.

## Is Apple Finally Changing The Name of OS X?

Apple seems to be in the process of renaming one of its most important products, as evidenced by the wording of some documentation added to the company s website yesterday. The text of a now-amended FAQ page about Apple s relationship with the environment initially referred to Mac OS X as MacOS, prompting speculation that a rebranding is in the works.

For well over a decade, OS X has been the name for the operating system used on millions of Macs around the world  but it s fair to say that Apple has changed a lot since the OS was implemented in 2002. This minor edit would bring its moniker in line with the likes of iOS, tvOS, and watchOS.

This isn t the first indication that Apple might be mulling such a change. Last month, the term  macOS  was found in the name of a file included in the OS X 10.11.4 update which was distributed to users on March 21, as referenced in reporting by 9to5Mac.

Of course, there is a minor difference between these two pieces of evidence; one capitalizes the word Mac, whereas the other does not. The lower-case style certainly fits the pattern of Apple s other platforms, but it also makes sense that the company would continue to treat the word Mac as a proper noun.

Regardless, the fact that the software development team and the copywriter behind the FAQ page both seem to be familiar with the label MacOS seems to suggest that the rebranding is common knowledge in the halls of Apple HQ. It remains to be seen how long it ll be before we hear official word from Apple on the situation.

Since the release of OS X 10.7 in 2011, Apple has stuck to an annual schedule for the launch of its incremental updates. If OS X is indeed set to transform into MacOS, we can perhaps expect the announcement to be made when the next version is unveiled to the public  which will likely take place in the fall.

## Apple Might ve Let  MacOS  Rebranding for OS X Slip Out

Evidence that Apple will rebrand OS X to MacOS is starting to pile up, with the new name appearing briefly on Apple s own website.

As spotted by 9to5Mac, Apple s Environment page got an update on Thursday, and for a short time it included a reference to MacOS.  Years of use, which are based on first owners, are assumed to be four years for MacOS and tvOS devices and three years for iOS and watchOS devices,  the page said. (Apple has since reverted the name to OS X.)

This isn t the first time the potential name change has slipped out. Last month, an Interface Builder document inside the OS X system folder included a file named  FUFlightViewController_macOS.nib  (emphasis ours). Still,

9to5Mac noted that the name could have been included for the sake of convenience, as developers sometimes prefer the symmetry of iOS and macOS suffixes together. The name s appearance on an official webpage seems like strong evidence.

Also worth noting: Last June, Apple marketing head Phil Schiller vaguely hinted at more name changes to come, after the company announced watchOS for the Apple Watch. I think, you ll see. Give us time, we ve been through many fun naming things, Schiller told John Gruber during a live podcast at Apple s WWDC conference. (At the time, however, Apple still hadn t revealed tvOS for the Apple TV.)

Why this matters: A name change would make sense given that all of Apple s other operating systems now fall under the [prefix]OS naming scheme. And given that Apple has been updating the desktop version of OS X for more than 15 years now, the roman numeral for 10 has long outlived its functional purpose. MacOS or, perhaps, macOS could be a fun throwback to the operating system s origins, while positioning it for the future alongside Apple s broadening range of phones, tablets, watches, and TV devices.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.